Gates & Cooper LLP

Howard Hughes Center
6701 Center Drive West, Suite 1050
Los Angeles, California 90045

FAX TRANSMISSION TO USPTO

TO: Commissioner for Patents
MS: REPLY BRIEF - PATENTS
Patent Examining Corps
Facsimile Center
Alexandria, VA 22313-1450

FROM: George H. Gates
OUR REF.: ARC9-98-125
TELEPHONE: (310) 642-4146

Total pages, including cover letter: 16

PTO FAX NUMBER: 703/872-9306

If you do NOT receive all of the pages, please telephone us at (310) 641-8797, or fax us at (310) 641-8798.

Title of Document Transmitted:	**REPLY BRIEF OF APPELLANTS.**
Applicant:	Kevin S. McCurley et al.
Serial No.:	09/260,448
Filed:	March 2, 1999
Group Art Unit:	2131
Title:	SECURE USER-LEVEL TUNNELS ON THE INTERNET
Our Ref. No.:	ARC9-98-125

Please charge all requisite fees to Deposit Account No. 09-0441 of IBM Corporation, the assignee of the present application.

By: _____
Name: George H. Gates
Reg. No.: 33,500

I hereby certify that this paper is being transmitted by facsimile to the U.S. Patent and Trademark Office on the date shown below.

_____
Signature

Dec. 1, 2004
Date

GHG/io

G&C 30879.64-US-01

Due Date: December 1, 2004

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Kevin S. McCurley et al.	Examiner:	Christopher A. Revak
Serial No.:	09/260,448	Group Art Unit:	2131
Filed:	March 2, 1999	Docket:	ARC9-98-125
Title:	SECURE USER-LEVEL TUNNELS ON THE INTERNET		

CERTIFICATE OF MAILING OR TRANSMISSION UNDER 37 CFR 1.8

I hereby certify that this correspondence is being filed via facsimile transmission to the U.S. Patent and Trademark Office on December 1, 2004.

By:
Name: George H. Gates

Mail Stop REPLY BRIEF - PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

We are transmitting herewith the attached:

☒ Transmittal sheet, in duplicate, containing a Certificate of Mailing or Transmission under 37 CFR 1.8.
☒ Reply Brief of Appellants.

Please consider this a PETITION FOR EXTENSION OF TIME for a sufficient number of months to enter these papers, if appropriate.

Please charge all fees to Deposit Account No. 09-0441 of IBM Corporation, the assignee of the present application. A duplicate of this paper is enclosed.

Customer Number 22462

GATES & COOPER LLP
Howard Hughes Center
6701 Center Drive West, Suite 1050
Los Angeles, CA 90045
(310) 641-8797

By:
Name: George H. Gates
Reg. No.: 33,500
GHG/io

Due Date: December 1, 2004

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Kevin S. McCurley et al.	Examiner:	Christopher A. Revak
Serial No.:	09/260,448	Group Art Unit:	2131
Filed:	March 2, 1999	Docket:	ARC9-98-125
Title:	SECURE USER-LEVEL TUNNELS ON THE INTERNET		

CERTIFICATE OF MAILING OR TRANSMISSION UNDER 37 CFR 1.8

I hereby certify that this correspondence is being filed via facsimile transmission to the U.S. Patent and Trademark Office on December 1, 2004.

By: _____
Name: George H. Gates

Mail Stop REPLY BRIEF - PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

We are transmitting herewith the attached:

☒ Transmittal sheet, in duplicate, containing a Certificate of Mailing or Transmission under 37 CFR 1.8.
☒ Reply Brief of Appellants.

Please consider this a PETITION FOR EXTENSION OF TIME for a sufficient number of months to enter these papers, if appropriate.

Please charge all fees to Deposit Account No. 09-0441 of IBM Corporation, the assignee of the present application. A duplicate of this paper is enclosed.

Customer Number 22462

GATES & COOPER LLP
Howard Hughes Center
6701 Center Drive West, Suite 1050
Los Angeles, CA 90045
(310) 641-8797

By: _____
Name: George H. Gates
Reg. No.: 33,500
GHG/io

G&C 30879.64-US-01

Due Date: December 1, 2004

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of:	
Inventor: Kevin S. McCurley et al.	Examiner: Christopher A. Revak
Serial #: 09/260,448	Group Art Unit: 2131
Filed: March 2, 1999	Appeal No.: _____
Title: SECURE USER-LEVEL TUNNELS ON THE INTERNET	

REPLY BRIEF OF APPELLANTS

Commissioner for Patents
P. O. Box 1450
Alexandria, Virginia 22313-1450

Dear Sir:

I. Introduction

In accordance with 37 CFR §41.37, Appellants' attorney hereby submits the Reply Brief of Appellants, in response to the Examiner's Answer dated October 1, 2004 in the above-identified application.

This Reply Brief of Appellants incorporates by reference herein the entirety of the previously filed Brief of the Appellants.

No fee is required for filing this Reply Brief. However, the Office is authorized to charge any necessary fees or credit any overpayments to Deposit Account No. 09-0441 of IBM Corporation, the assignee of the present invention.

II. Arguments

In the Answer, the Examiner first states, on page 3, that Fryer et al., "Microsoft Press Computer Dictionary," was cited to show the use of UDP (User Datagram Protocol) and also for evidence of the definition of multiplexing and how it is used. The Examiner asserts that pp. 320 of Fryer et al. was cited to show that the Examiner's interpretation is consistent with that which

is known in the prior art. Moreover, the Examiner asserts that Appellants only mentioned pp. 482 that shows the use of UDP in their brief and have not commented on pp. 320 of Fryer et at that recites of multiplexing.

Appellants' attorney does not dispute the definition of "multiplexing," as found in the Fryer et al. reference. What Appellants' attorney does dispute is the Examiner's assertion that the combination of references teach or suggest multiplexing in the same context as recited in Appellants' claims, namely multiplexing other connections through a secure connection established over a single Transmission Control Protocol (TCP) connection. More arguments in this regard are provided below.

Thereafter, the Examiner sets forth a number of responses to the Brief of Appellants. Specifically, at pages 5 et seq. of the Answer, the Examiner states the following:

> (II) Response to Argument Appellant's arguments:
> The appellant has argued on page 12 of the brief that the combination of references does not teach or suggest (a) opening a single Transmission Control Protocol (TCP) connection are a user-level between at least two endpoints in the network, (b) establishing a secure connection using Secure Socket Layer (SSL) over the opened Transmission Control Protocol (TCP) connection, (c) mutually authenticating each of the endpoints of the secure connection, and (d) multiplexing other connections through the secure connection once both of the endpoints have been authenticated, wherein either endpoint of the secure connection can receive connection requests for the multiplexed other connections.
> Furthermore, the appellant argues that the combination of references does not teach or suggest that either of the endpoints of the secure connection can receive connection requests, in the context of a single Transmission Control Protocol (TCP) connection as a user-level between the endpoints, where a secure connection using Secure Socket Layer (SSL) has been established over where other connections are multiplexing through the secure connection once both of the endpoints have been authenticated.
> The examiner respectfully disagrees for the following reasons:
> As per the appellant's "opening a single Transmission Control Protocol (TCP) connection at a user level between two endpoints" and "establishing a secure connection using Secure Socket Layer (SSL) over the opened Transmission Control Protocol (TCP) connection," the examiner directs the appellant to Freier et al whereby it is disclosed that "at a lowest level, layered on top of some reliable transport protocol (e.g., TCP), is the SSL protocol" as is recited on page 3, section 1 entitled Introduction. Freier et al further recites that "The SSL protocol is designed to establish a secure connection between the client and a server communicating over an insecure channel as is recited on page 54, section F entitled Security Analysis. Freier's use of "a secure connection" is interpreted as a single connection since it is recited in singular form. Since Freier

discloses that SSL is used on top of TCP, the TCP connection is already opened and is being used as is taught Freier et al. Weinstein provides further support for use of "opening a TCP connection" and "opened TCP connection" by disclosing that "SSL is layered on top of some reliable transport protocol (TCP)" and when a user desires to establish a connection to the server, the client first initiates a connection to the server, please refer to column 3, lines 6-8 and column 4, lines 52-53 of Weinstein. Similar to Freier, Weinstein again shows that the TCP connection is initially opened and stays open for the SSL session. The user, or user level, uses the client computer to initiate, establish, and open this TCP connection. In summary, the SSL connection is used on the TCP connection that uses it protocol to first establish the connection between the client and server, at the user's request, then goes through the SSL protocol to establish the SSL connection. The SSL connection is argued below.

The appellant has argued that the prior art of record does not teach "mutually authenticating each of the endpoints of the secure connection." The examiner disagrees for it is disclosed by Freier et al that SSL authenticates a server with a client and client with a server, see page 3, section 1 entitled Introduction and page 54, section F.1.1, entitled Authentication and Key Exchange. Since they are both authenticated to each other, the authentication process is mutual since they need to authenticate each other in order to establish a common key used for encrypting the SSL connection. The examiner additionally notes that this limitation of "mutually authenticating" is not claimed in independent claims 1 and 40, it is only recited in independent claim 79. The language of "each of the devices authenticates the other device" is broader than "mutually authenticating," wherein Freier et al recites of both instances in the disclosure to meet the appellant's claim language.

The appellant argues that "multiplexing other connections through the secure connection once both of the endpoints have been authenticated, wherein either endpoint of the secure connection can receive connection requests for the multiplexed other connections" has not been disclosed by the prior art combination. The examiner respectfully disagrees, it is disclosed by Freier et al of "an SSL session may include multiple secure connections, in addition, parties may have multiple simultaneous sessions" as is recited on pages 9-10, section 5.1 entitled Session and Connection States. The examiner relied upon Fryer et al to show that "multiplexing is defined as a technique used in communications and input/output operations for transmitting a number of separate signals simultaneously over a single channel or line" as is recited on page 320. The examiner has already argued and established evidence of a single connection as is argued above in light of the teachings of both Freier et al and Weinstein. Since Freier et al recites of multiple secure sessions and multiple simultaneous sessions, the examiner contends that multiplexing is used in the teachings of Freier et al based upon the evidence disclosed in Fryer et al. The argument of "either endpoint of the secure connection can receive connection requests" is relied upon by the teachings of Weinstein. Weinstein discloses when a user desires to establish a connection to the server, the client first initiates a connection to the server, please refer to column 3, lines 6-8 and column 4, lines 52-53. It is further

> taught that either the client or server, equivalent to endpoints, are able to receive data or connection requests, please refer to column 2, lines 23-34 and column 8, lines 38-44 & 53-61. This passages show that Weinstein is capable of either endpoint being able to receive connection requests.
>
> In summary, the examiner has found the teachings of Freier et al and Weinstein belong to the same endeavor and field of scope as that of the appellant's. The examiner has found no distinction between the prior art of record as compared to the appellant's claim language. For the above reasons, it is believed that the rejections should be sustained.

Appellants' attorney disagrees.

Appellants' invention, as recited in independent claims 1, 40 and 79, is patentable over the references, because the claims recite a specific combination of limitations not found in the references. Specifically, the references do not teach or suggest the specific sequence of steps comprising: (a) opening a single Transmission Control Protocol (TCP) connection at a user-level between at least two endpoints in the network; (b) establishing a secure connection using Secure Sockets Layer (SSL) over the opened Transmission Control Protocol (TCP) connection; (c) mutually authenticating each of the endpoints of the secure connection; and (d) multiplexing other connections through the secure connection once both of the endpoints have been authenticated, wherein either endpoint of the secure connection can receive connection requests for the multiplexed other connections.

The Examiner cites Freier as teaching "opening a single Transmission Control Protocol (TOP) connection at a user level between two endpoints" and "establishing a secure connection using Secure Socket Layer (SSL) over the opened Transmission Control Protocol (TCP) connection," at page 3, section 1 entitled Introduction, and page 54, section F entitled Security Analysis.

> Freier: page 3, Section 1
> 1. Introduction
>
> The primary goal of the SSL Protocol is to provide privacy and reliability between two communicating applications. The protocol is composed of two layers. At the lowest level, layered on top of some reliable transport protocol (e.g., TCP[TCP]), is the SSL Record Protocol. The SSL Record Protocol is used for encapsulation of various higher level protocols. One such encapsulated protocol, the SSL Handshake Protocol, allows the server and client to authenticate each other and to negotiate an encryption algorithm

and cryptographic keys before the application protocol transmits or receives its first byte of data. One advantage of SSL is that it is application protocol independent. A higher level protocol can layer on top of the SSL Protocol transparently. The SSL protocol provides connection security that has three basic properties:

- The connection is private. Encryption is used after an initial handshake to define a secret key. Symmetric cryptography is used for data encryption (e.g., DES[DES], RC4[RC4], etc.)
- The peer's identity can be authenticated using asymmetric, or public key, cryptography (e.g., RSA[RSA], DSS[DSS], etc.).
- The connection is reliable. Message transport includes a message integrity check using a keyed MAC. Secure hash functions (e.g., SHA, MD5, etc.) are used for MAC computations.

Freier: page 54, Section F

F. Security analysis

The SSL protocol is designed to establish a secure connection between a client and a server communicating over an insecure channel. This document makes several traditional assumptions, including that attackers have substantial computational resources and cannot obtain secret information from sources outside the protocol. Attackers are assumed to have the ability to capture, modify, delete, replay, and otherwise tamper with messages sent over the communication channel. This appendix outlines how SSL has been designed to resist a variety of attacks.

The Examiner cites Weinstein as teaching "opening a TCP connection" and "opened TCP connection" by disclosing that "SSL is layered on top of some reliable transport protocol (TCP)" and when a user desires to establish a connection to the server, the client first initiates a connection to the server, at column 3, lines 6-8 and column 4, lines 52-53.

Weinstein: Col. 3, lines 6-8 (actually lines 4-21)

The process of the SSL step up is described in FIG. 1. The process involves performing an SSL handshake twice. The process begins (100) when a user desires to establish a session with a server. The client first initiates a network connection to the server (110). The first handshake between an export client and an approved server results in an SSL session that uses export strength encryption (120). This establishes a connection using an exportable cipher suite (130). The client examines the server's certificate obtained as part of the first handshake (140). If the server is not approved, the SSL session transfers application data that are protected by the export cipher (180). If the server is approved, then the client

initiates a second handshake (150), this time allowing stronger cipher suites. The result of the second handshake is an SSL session that uses strong encryption (160). The SSL session may then be used to transfer application data that are protected by the strong cipher suite (170). At this point, the step up process is complete (190).

Weinstein: Col. 4, lines 52-53 (actually lines 49-62)

The primary goal of the SSL Protocol is to provide privacy and reliability between two communicating applications. The protocol is composed of two layers. At the lowest level, layered on top of some reliable transport protocol (e.g. TCP), is the SSL Record Protocol. The SSL Record Protocol is used for encapsulation of various higher level protocols. One such encapsulated protocol, the SSL Handshake Protocol, allows the server and client to authenticate each other and to negotiate an encryption algorithm and cryptographic keys before the application protocol transmits or receives its first byte of data. One advantage of SSL is that it is application protocol independent. A higher level protocol can layer on top of the SSL Protocol transparently.

The Examiner cites Freier as teaching "mutually authenticating each of the endpoints of the secure connection" by disclosing that SSL authenticates a server with a client and client with a server, at page 3, section 1 entitled Introduction and page 54, section F.1.1, entitled Authentication and Key Exchange.

Freier: page 3, Section 1

1. Introduction

The primary goal of the SSL Protocol is to provide privacy and reliability between two communicating applications. The protocol is composed of two layers. At the lowest level, layered on top of some reliable transport protocol (e.g., TCP[TCP]), is the SSL Record Protocol. The SSL Record Protocol is used for encapsulation of various higher level protocols. One such encapsulated protocol, the SSL Handshake Protocol, allows the server and client to authenticate each other and to negotiate an encryption algorithm and cryptographic keys before the application protocol transmits or receives its first byte of data. One advantage of SSL is that it is application protocol independent. A higher level protocol can layer on top of the SSL Protocol transparently. The SSL protocol provides connection security that has three basic properties:

- The connection is private. Encryption is used after an initial handshake to define a secret key. Symmetric cryptography is used for data encryption (e.g., DES[DES], RC4[RC4], etc.)

- The peer's identity can be authenticated using asymmetric, or public key, cryptography (e.g., RSA[RSA], DSS[DSS], etc.).
- The connection is reliable. Message transport includes a message integrity check using a keyed MAC. Secure hash functions (e.g., SHA, MD5, etc.) are used for MAC computations.

Freier: page 49, Section F.1.1
F.1.1 Authentication and key exchange

SSL supports three authentication modes: authentication of both parties, server authentication with an unauthenticated client, and total anonymity. Whenever the server is authenticated, the channel should be secure against man-in- the-middle attacks, but completely anonymous sessions are inherently vulnerable to such attacks. Anonymous servers cannot authenticate clients, since the client signature in the certificate verify message may require a server certificate to bind the signature to a particular server. If the server is authenticated, its certificate message must provide a valid certificate chain leading to an acceptable certificate authority. Similarly, authenticated clients must supply an acceptable certificate to the server. Each party is responsible for verifying that the other's certificate is valid and has not expired or been revoked.

The general goal of the key exchange process is to create a pre_master_secret known to the communicating parties and not to attackers. The pre_master_secret will be used to generate the master_secret (see Section 6.1). The master_secret is required to generate the finished messages, encryption keys, and MAC secrets (see Sections 5.6.9 and 6.2.2). By sending a correct finished message, parties thus prove that they know the correct pre_master_secret.

The Examiner cites Freier as teaching "multiplexing other connections through the secure connection once both of the endpoints have been authenticated, wherein either endpoint of the secure connection can receive connection requests for the multiplexed other connections," by disclosing "an SSL session may include multiple secure connections, in addition, parties may have multiple simultaneous sessions," at pages 9-10, section 5.1 entitled Session and Connection States.

Freier: pages 9-10, Section 5.1

5.1 Session and connection states

An SSL session is stateful. It is the responsibility of the SSL Handshake protocol to coordinate the states of the client and server, thereby allowing the protocol state machines of each to operate consistently, despite the fact that the state is not exactly parallel. Logically the state is represented twice, once as the current operating state, and (during the handshake protocol) again as the pending state. Additionally, separate read and write states are maintained. When the client or server receives a change cipher spec message, it copies the pending read state into the current read state. When the client or server sends a change cipher spec message, it copies the pending write state into the current write state. When the handshake negotiation is complete, the client and server exchange change cipher spec messages (see Section 5.3), and they then communicate using the newly agreed-upon cipher spec.

An SSL session may include multiple secure connections; in addition, parties may have multiple simultaneous sessions.

The session state includes the following elements:

session identifier
: An arbitrary byte sequence chosen by the server to identify an active or resumable session state.

peer certificate
: X509.v3[X509] certificate of the peer. This element of the state may be null.

compression method
: The algorithm used to compress data prior to encryption.

cipher spec
: Specifies the bulk data encryption algorithm (such as null, DES, etc.) and a MAC algorithm (such as MD5 or SHA). It also defines cryptographic attributes such as the hash_size. (See Appendix A.7 for formal definition)

master secret
: 48-byte secret shared between the client and server.

is resumable
: A flag indicating whether the session can be used to initiate new connections.

The connection state includes the following elements:

server and client random
: Byte sequences that are chosen by the server and client for each connection.

server write MAC secret
: The secret used in MAC operations on data written by the server

client write MAC secret

> The secret used in MAC operations on data written by the client.
>
> server write key The bulk cipher key for data encrypted by the server and decrypted by the client.
>
> client write key The bulk cipher key for data encrypted by the client and decrypted by the server.
>
> initialization vectors
>
> When a block cipher in CBC mode is used, an initialization vector (IV) is maintained for each key. This field is first initialized by the SSL handshake protocol. Thereafter the final ciphertext block from each record is preserved for use with the following record.
>
> sequence numbers Each party maintains separate sequence numbers for transmitted and received messages for each connection. When a party sends or receives a change cipher spec message, the appropriate sequence number is set to zero. Sequence numbers are of type uint64 and may not exceed 2^64-1.

The Examiner relies upon Fryer to show that "multiplexing is defined as a technique used in communications and input/output operations for transmitting a number of separate signals simultaneously over a single channel or line," at page 320.

> Fryer: page 320
>
> A technique used in communications and input/output operations for transmitting a number of separate signals simultaneously over a single channel or line.

According to the Examiner, since Freier recites multiple secure sessions and multiple simultaneous sessions, multiplexing is used in Freier based upon the evidence disclosed in Fryer.

The Examiner cites Weinstein as teaching "either endpoint of the secure connection can receive connection requests," because it discloses when a user desires to establish a connection to the server, the client first initiates a connection to the server, at column 3, lines 6-8 and column 4, lines 52-53.

> Weinstein: Col. 3, lines 6-8 (actually lines 4-21)
>
> The process of the SSL step up is described in FIG. 1. The process involves performing an SSL handshake twice. The process begins (100) when a user desires to establish a session with a server. The client first initiates a network connection to the server (110). The first handshake between an export client and

an approved server results in an SSL session that uses export strength encryption (120). This establishes a connection using an exportable cipher suite (130). The client examines the server's certificate obtained as part of the first handshake (140). If the server is not approved, the SSL session transfers application data that are protected by the export cipher (180). If the server is approved, then the client initiates a second handshake (150), this time allowing stronger cipher suites. The result of the second handshake is an SSL session that uses strong encryption (160). The SSL session may then be used to transfer application data that are protected by the strong cipher suite (170). At this point, the step up process is complete (190).

Weinstein: Col. 4, lines 52-53 (actually lines 49-62)

The primary goal of the SSL Protocol is to provide privacy and reliability between two communicating applications. The protocol is composed of two layers. At the lowest level, layered on top of some reliable transport protocol (e.g. TCP), is the SSL Record Protocol. The SSL Record Protocol is used for encapsulation of various higher level protocols. One such encapsulated protocol, the SSL Handshake Protocol, allows the server and client to authenticate each other and to negotiate an encryption algorithm and cryptographic keys before the application protocol transmits or receives its first byte of data. One advantage of SSL is that it is application protocol independent. A higher level protocol can layer on top of the SSL Protocol transparently.

The Examiner cites Weinstein as teaching that either the client or server, equivalent to endpoints, are able to receive data or connection requests, at column 2, lines 23-34 and column 8, lines 38-44 and 53-61.

Weinstein: Col. 2, lines 23-34

SSL Client: The software that initiates the SSL handshake and performs the client side of the handshake protocol. This software could be part of either a client or server product.

SSL Server: The software that performs the server side of the SSL handshake protocol. This software could be part of either a client or server product, but is generally part of a server product.

Negotiate/Handshake: The process by which an SSL client and server agree upon a set of encryption and authentication algorithms, and exchange the data necessary to initiate those algorithms.

Weinstein: col. 8, lines 38-44

SSL is a layered protocol. At each layer, messages may include fields for length, description, and content. SSL takes messages to be transmitted, fragments the data into manageable blocks, optionally compresses the data, applies a MAC, encrypts, and transmits the result. Received data are decrypted, verified, decompressed, and reassembled, then delivered to higher level clients.

> Weinstein: col. 8, lines 53-61 (actually lines 46-61)
> An SSL session is stateful. It is the responsibility of the SSL handshake protocol to coordinate the states of the client and server, thereby allowing the protocol state machines of each to operate consistently, despite the fact that the state is not exactly parallel. Logically the state is represented twice, once as the current operating state, and (during the handshake protocol) again as the pending state. Additionally, separate read and write states are maintained. When the client or server receives a change cipher spec message, it copies the pending read state into the current read state. When the client or server sends a change cipher spec message, it copies the pending write state into the current write state. When the handshake negotiation is complete, the client and server exchange change cipher spec messages, and then communicate using the newly agreed upon cipher spec.

Appellants' attorney respectfully asserts that the combination of the above references does not teach or suggest (a) opening a single Transmission Control Protocol (TCP) connection at a user-level between at least two endpoints in the network, (b) establishing a secure connection using Secure Sockets Layer (SSL) over the opened Transmission Control Protocol (TCP) connection, (c) mutually authenticating each of the endpoints of the secure connection, and (d) multiplexing other connections through the secure connection once both of the endpoints have been authenticated, wherein either endpoint of the secure connection can receive connection requests for the multiplexed other connections.

Instead, Freier merely describes SSL sessions, states that an SSL session may include multiple secure connections and multiple simultaneous sessions, describes SSL's authentication modes, and states that the SSL Record Protocol as being layered on top of a transport protocol such as TCP. Similarly, Weinstein merely describes SSL as a layered protocol and an SSL session as stateful. Finally, Fryer merely defines multiplexing.

While Freier describes how an SSL session may include multiple secure connections and multiple simultaneous sessions, nowhere does Freier, or any of the other references, teach or suggest a single Transmission Control Protocol (TCP) connection at a user-level between the endpoints, where a secure connection using Secure Sockets Layer (SSL) has been established over the opened TCP connection, where each of the endpoints have been mutually authenticated, and where other connections are multiplexed through the secure connection once both of the endpoints have been authenticated. Moreover, none of the references teach that either of the endpoints of a secure connection using SSL over a single TCP connection can receive connection requests so that other connections are multiplexed through the connection.

The remaining references fail to overcome the deficiencies of Freier, Weinstein and Fryer. For example, Griffiths was cited merely for resolving domain names; Netscape was cited merely for describing the use of SOCKS as a means for accessing information on the Internet; Coley was cited merely for using a bastion firewall host computer; and Raz was cited merely for using multiple Intranets.

Moreover, the various elements of Appellants' claimed invention together provide operational advantages over the cited references. In addition, Appellants' invention solves problems not recognized by the cited references.

Thus, Appellants' attorney submits that independent claims 1, 40 and 79 are allowable over the cited references. Further, dependent claims 2-3, 5-39, 41-42, 44-78, 80-81 and 83-117 are submitted to be allowable over the cited references in the same manner, because they are dependent on independent claims 1, 40 and 79, respectively, and thus contain all the limitations of the independent claims.

In addition, dependent claims 2-3, 5-39, 41-42, 44-78, 80-81 and 83-117 recite additional novel elements not shown by the cited references. More specifically, the references do not teach or suggest the limitations of dependent claims 2-3, 5-39, 41-42, 44-78, 80-81 and 83-117 in the same context as Appellants' invention.

III. Conclusion

In light of the above arguments, Appellants' attorney respectfully submits that the cited reference does not anticipate nor render obvious the claimed invention. More specifically, Appellants' claims recite novel functions and features which patentably distinguish over any and all references under 35 U.S.C. §§ 102 and 103.

As a result, a decision by the Board of Patent Appeals and Interferences reversing the Examiner and directing allowance of the pending claims in the subject application is respectfully solicited.

Respectfully submitted,

Appellants' attorneys,

GATES & COOPER LLP

Howard Hughes Center
6701 Center Drive West, Suite 1050
Los Angeles, California 90045
(310) 641-8797

Date: December 1, 2004

By: _____
Name: George H. Gates
Reg. No.: 33,500

GHG/